TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

October 2002

Reference Number: 2003-20-019

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

October 26, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J Gardiner

FROM: Pamela J. Gardiner
Acting Inspector General

SUBJECT: Final Audit Report – Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices (Audit # 200220025)

This report presents the results of our review of the effectiveness and consistency of selected computer security controls in Internal Revenue Service (IRS) field offices. In each office, we determined whether selected SANS/FBI Top Twenty vulnerabilities[1] existed. We also tested for additional vulnerabilities suggested by our contractor.[2] These vulnerabilities are widely known in the cyber-security industry and to hackers.

In summary, computer security controls were not implemented effectively in most of the offices we visited, and a wide range in the number of vulnerabilities existed between offices. The vulnerabilities identified could be exploited by disgruntled employees and by hackers to access data, change data, or to obtain information for a denial of service attack.[3]

For example, some offices installed operating systems using default settings that are well known by hackers instead of modifying the settings. A default installation would allow an anonymous user with no password to obtain a listing of user account names. Some accounts did not have a user profile which is needed to restrict access for each user. Another illustration of a potential vulnerability included accounts with passwords

[1] The SANS/FBI Top Twenty list, released on October 1, 2001, shows common security flaws that account for a majority of successful attacks. This list expands on last year's list, "Ten Most Critical Internet Security Vulnerabilities," which was released by SANS and the National Infrastructure Protection Center (NIPC). See http://www.sans.org for additional information.

[2] See Appendix IV for a general listing of vulnerabilities by category.

[3] A denial of service attack occurs when an intruder takes over the resources of a system to limit access of legitimate users to the system.

that were marked “never expire” or “cannot change.” Over time, the chances for disclosure or abuse of a permanent password are high.

Of the six offices we tested, San Francisco and Oakland had a higher rate of vulnerabilities for both Windows NT servers and workstations. The New Carrollton Federal Building and Atlanta had lower rates of vulnerabilities for both servers and workstations. The other offices had mixed results. Vulnerabilities were identified and recommended corrective actions were provided by the commercial software reports. Test results were provided to local IRS managers in each of the offices we visited for assessment and appropriate corrective action.

Systems administrators have the responsibility for ensuring the proper protection of system software. We contacted systems administrators for each of the offices visited to identify some of the possible causes for not implementing security controls effectively and consistently. A variety of reasons were provided including operational demands, budgetary constraints, lack of resources, and equipment being replaced or relocated.

Of particular importance, however, was the lack of computer security training. As of May 2002, none of the six systems administrators we contacted had received any security training within this calendar year, and five had not received any security training in the prior calendar year. Also, existing IRS guidance covering system administrator responsibilities does not explicitly state what responsibility they have in regard to patching software. This lack of guidance could lessen the accountability and responsibility for ensuring that IRS systems are properly protected and maintained.

We recommend that systems administrators responsible for the equipment in the offices we tested be given security training tailored to mitigating vulnerabilities identified in the SANS/FBI Top Twenty list. An assessment of whether adequate security training has been provided to systems administrators in other offices should also be considered.

Management’s Response: The Chief, Security Services, concurred with our recommendation and indicated that activities are underway to identify, define, and develop security training within the next 18 months, barring any shift of resources. Management’s complete response to the draft report is included as Appendix V.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, “Limited Official Use Information and Other Legends” of the Department of Treasury Security Manual. Because this document has been designated Limited Official Use, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA’s Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendation. Please contact me at (202) 622-6510 if you have questions or

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

Background

The Internal Revenue Service's (IRS) network is an outgrowth of a large number of local area networks developed and installed by data communication technicians and architects from various offices located throughout the country. Ensuring that security controls are implemented effectively and consistently in a widely dispersed organization like the IRS is clearly a challenge.

Systems administrators are charged with the responsibility to ensure proper protection and use of system software. The End User Equipment and Service Group, the Domain Infrastructure Networking Group, and the Office of Mission Assurance also share responsibility for providing guidance, testing, and implementation.

We performed this audit to meet the requirements of the IRS Restructuring and Reform Act of 1998,[1] which requires the Treasury Inspector General for Tax Administration (TIGTA) to annually assess the security of IRS technology. The audit work was performed from January through August 2002. We conducted our network vulnerability tests in Atlanta, Georgia (Summit Building); Newark, New Jersey (Broad Street); Lanham, Maryland (New Carrollton Federal Building); Philadelphia, Pennsylvania (Arch Street); and San Francisco, California (Golden Gate Avenue).

This audit was performed in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Security Controls Were Not Implemented Effectively and Consistently

Computer security controls were not implemented effectively in most of the offices we visited, and a wide range in the number of vulnerabilities existed between offices. The vulnerabilities identified could be exploited to

[1] Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

access data, change data, or to obtain information for use in a denial of service attack.[2]

For example, some offices installed operating systems using default settings that are well known by hackers instead of modifying the settings. A default installation would allow an anonymous user without a password to obtain a listing of user account names.

Some accounts did not have a user profile. User profiles provide security on network systems because they are designed to restrict access for each user. Guest accounts were usually disabled, but two instances were found where the Guest account was enabled. This would provide an intruder who logged in as Guest to have expanded access to the network.

Another illustration of a potential vulnerability included accounts with passwords that were marked "never expire" or "cannot change." Over a period of time, the chances for disclosure or abuse of a permanent password are high. A complete list of the vulnerability categories for which we tested is included in Appendix IV.

The vulnerabilities identified are exploitable from within the IRS' network. Many security experts view insider threats as the most dangerous and hardest to detect.[3] The most devastating threats to security have come from individuals who were deemed trusted insiders. Additionally, should perimeter controls such as firewalls and intrusion detection systems be breached, an external hacker could take advantage of the same vulnerabilities.

We provided each office we visited the results generated by our software (Internet Security Systems (ISS) ™ Internet Scanner) for assessment and corrective action as appropriate. The results included the identification and

[2] A denial of service attack occurs when an intruder takes over the resources of a system to limit access of legitimate users to the system.
[3] For a discussion of the insider threat see the Texas A&M Research Foundation's web site at: http://rf-web.tamu.edu/files/SECGUIDE/V1comput/Threats.htm#Threats

description of vulnerabilities and recommended corrective actions for identified vulnerabilities. Table 1 below represents the number of vulnerabilities identified by office and type of computer.[4]

Table 1. Number of Vulnerabilities by Office and Device Type

Office Location	Windows NT Servers	Windows NT Work-Stations	Unix Servers	Unix Work-stations	Routers	Web Servers
Atlanta, GA	7	55	7	N/A	1	N/A
Newark, NJ (Including Springfield)	51	19	N/A	N/A	N/A	N/A
Lanham, MD	12	21	N/A	N/A	1	8
Oakland, CA	30	45	8	7	1	11
Philadelphia, PA	25	97	7	N/A	1	3
San Francisco, CA	45	57	7	7	N/A	N/A

Prepared by: TIGTA, May 2002 N/A= Not Applicable

Approximately 87 percent of all vulnerabilities found by office are from Windows NT workstations (55 percent) and Windows NT servers (32 percent). The remaining 13 percent represent vulnerabilities in Unix-based systems, routers, and web servers. The vulnerabilities we identified were not isolated to any particular computer in the offices we visited.

The types and numbers of vulnerabilities varied widely among the offices tested

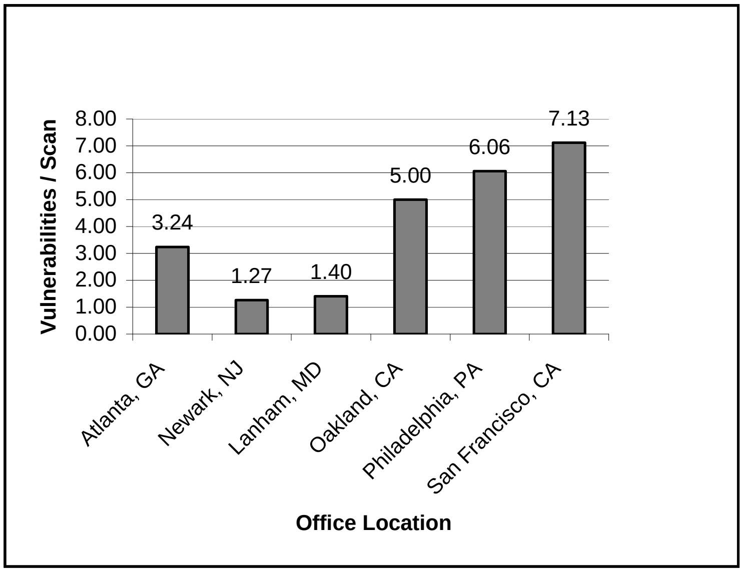
We found a wide range of vulnerabilities among the offices visited. Table 2 shows that the average number of vulnerabilities identified per Windows NT workstation ranged from 1.27 to 7.13. Table 3 shows the average number of vulnerabilities per Windows NT server varied

[4] See Appendix I, Table 1 for the number of devices and types tested by location.

from 1.00 to 9.00. Vulnerabilities per scan for Tables 2 and 3 were determined by dividing the number of vulnerabilities shown in Table 1 by the number of like computers scanned shown in Appendix I.

Table 2 shows the average number of vulnerabilities for each Windows NT workstation by office location.

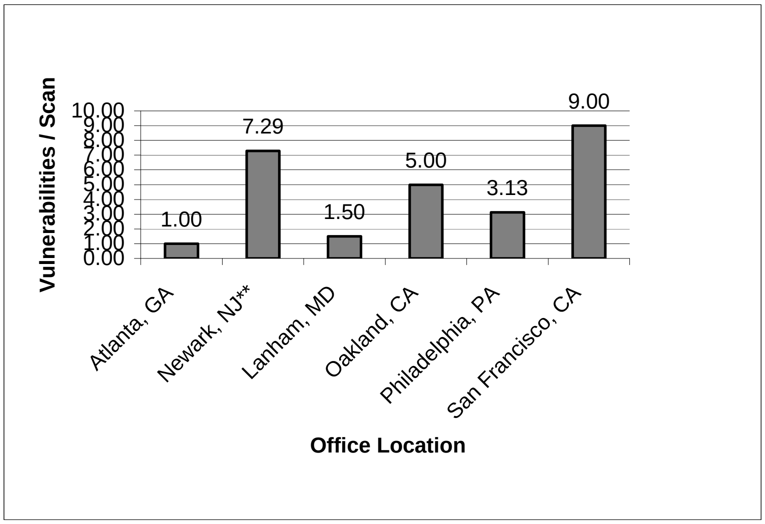
Table 2. Windows NT Workstations: Distribution of Unique Vulnerabilities per Workstation by Office



Source: TIGTA

Table 3 shows the average number of vulnerabilities for each Windows NT server by office location.

Table 3. Windows NT Servers: Distribution of Unique Vulnerabilities per Server by Office



Source: TIGTA **Servers located in Springfield, NJ

San Francisco and Oakland had a higher rate of vulnerabilities for both Windows NT servers and workstations. The New Carrollton Federal Building and Atlanta had lower rates of vulnerabilities for both servers and workstations. We attribute Atlanta’s and New Carrollton’s lower results to vigilant management practices. The other offices had mixed results.

The low vulnerabilities per scan for Newark Windows NT workstations can be explained because 7 of the 15 workstations tested had been updated with standard software known in the IRS as the Common Operating Environment (COE). Workstations updated with the COE had fewer vulnerabilities, which reduced the average number of vulnerabilities found per machine by office. The COE provides a means for the IRS to standardize its operating system and the various software applications on its workstations. The IRS plans to install the COE on over 100,000 workstations by 2004.

Systems administrators need additional training

We contacted six systems administrators from the offices we visited to determine the possible causes for the wide variation of vulnerabilities by office. A variety of reasons were provided including operational demands, budgetary constraints, the lack of resources, and equipment being replaced or relocated.

Of particular importance was the lack of computer security training. As of May 2002, none of the six systems administrators indicated they had received any security training this year and five had not received any security training in the prior calendar year.

We believe that had the systems administrators received training courses tailored to identifying and addressing common security vulnerabilities, such as those identified by the SANS/FBI Top Twenty list,[5] the number of vulnerabilities within and between offices could have been significantly reduced. The IRS, through its Cincinnati, Ohio training office, provides security-training courses. Perhaps this office could provide the training being recommended in this report.

Office of Management and Budget Circular A-130 Appendix III, the Computer Security Act of 1987,[6] and the Office of Personnel Management[7] all require that security training be provided.

A possible contributing factor for the variability between offices is that current IRS guidance does not explicitly state what role systems administrators should play in regards to software patches. For example, some systems

[5] The SANS/FBI Top Twenty list, released on October 1, 2001, shows common security flaws that account for a majority of successful attacks. This list expands on last year's list, "Ten Most Critical Internet Security Vulnerabilities," which was released by SANS and the National Infrastructure Protection Center (NIPC). See http://www.sans.org for additional information.

[6] See Public Law 100-235.

[7] See 5 C.F.R. § 930.301.

administrators were reluctant to apply patches without specific approval from Headquarters. This lack of guidance could lessen the accountability and responsibility for ensuring that an appropriate level of security is maintained over IRS systems.

Recommendation

The Deputy Commissioner for Modernization and Chief Information Officer should ensure that:

1. The system administrators responsible for the equipment in the offices we tested (see Appendix I, Table 1) are given appropriate security training tailored specifically to identifying, assessing, and addressing common security vulnerabilities such as those indicated on the SANS/FBI Top Twenty list. An assessment of whether adequate security training has been provided to systems administrators in other offices should also be considered.

Management's Response: The Chief, Security Services agreed with our recommendation. Barring any shift of resources, activities are underway to identify, define and develop security training in partnership with the Modernization, Information Technology and Security Services Embedded Learning and Education, Information Technology Services, and business units within the next 18 months.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness and consistency of security controls in Internal Revenue Service (IRS) offices. With contractor assistance from XACTA Corporation and using the SANS/FBI Top Twenty vulnerabilities[1] list, we identified specific vulnerabilities for Windows and Unix based systems for testing using Internet Security Systems (ISS) ™ Internet Scanner software.[2] Table 1 on the next page shows the number of systems tested by field office and device type.

The IRS officials located in their respective field office identified the devices to be tested using our original guidance for a sample size of 8 Windows NT servers, 10 to 15 Windows NT workstations, 2 routers including firewalls, and 2 Unix based systems. The number and types of devices tested was modified to accommodate the fact that not all field offices had the devices present or in the quantity sought.

We judgmentally selected six offices for review. In each of the offices, ISS software was used to identify the presence of these selected categories of vulnerabilities. These vulnerabilities are widely known in the cyber-security industry and to the hacker community.

The tests were conducted in January and February 2002. Appendix IV provides a brief description of the different categories of vulnerabilities for which we tested on IRS devices. As identified by the ISS software, the sub-objectives of this audit were to:

- Identify common weaknesses among selected sites and in sites with a high number of problems.
- Determine probable cause(s) of common weaknesses among selected sites and in specific sites with a high number of problems.

Methodology

Each test checked for the presence of a specific vulnerability. The table on the next page shows the number of the various types of devices that were tested in each location.

[1] The SANS/FBI Top Twenty list, released on October 1, 2001, shows common security flaws that account for a majority of successful attacks. This list expands on last year's list, "Ten Most Critical Internet Security Vulnerabilities," which was released by SANS and the National Infrastructure Protection Center (NIPC). See http://www.sans.org for additional information.

[2] See Appendix IV for a list of vulnerability categories.

Table 1. Number of Devices Tested By Location and Device Type

Office Locations	Windows NT Servers	Windows NT Workstations	Unix Based Servers	Unix Based Workstations	Routers	Web Servers
Atlanta, GA	7	17	2	0	2	0
Newark, NJ (Including Springfield)	7	15	0	0	0	0
Lanham, MD	8	15	0	0	2	1
Oakland, CA	6	9	2	1	1	1
Philadelphia, PA	8	16	2	0	1	1
San Francisco, CA	5	8	2	2	0	0

Sites tested:

- IRS Atlanta, 401 W. Peachtree NW (Summit Bldg), Atlanta, GA 30308
- IRS Newark, 970 Broad Street, Newark, NJ 07102
- IRS Washington, DC-Metro Area (New Carrollton Federal Building, Lanham, MD 20706)
- IRS Oakland, 1301 Clay Street, Oakland, CA 94612
- IRS Philadelphia, 600 Arch Street, Philadelphia, PA 19106
- IRS San Francisco, 450 Golden Gate Avenue, San Francisco, CA 94102

Note: Servers for Newark, NJ were located in Springfield, NJ. Tests conducted for the Oakland, CA office were performed from the San Francisco office.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Ted Grolimund, Acting Audit Manager
Bill Lessa, Senior Auditor
Midori Ohno, Senior Auditor
Stasha Smith, Senior Auditor
Ted Tomko, Senior Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Office of Security Services M:S
Chief, Information Technology Services M:I
Director, Embedded Learning and Education M:H
Director, Mission Assurance M:S:A
Director, End User Equipment & Services M:I:EU
Director, Financial Planning and Management M:I:F
Director, Enterprise Networks M:I:EN
Director, Web Services M:I:W
Director, Security Policy Support and Oversight M:S:S

Appendix IV

Categories of Vulnerabilities

For additional information on particular exploits, the SANS/FBI Top Twenty list can be accessed from the Internet at http://www.sans.org. To assist in the explanation of particular vulnerability categories, the SANS reference numbers are shown in parentheses. Additional vulnerabilities provided by XACTA Corporation, our contractor, are similarly noted.

General Vulnerabilities for both Unix and Windows Operating Systems

1. Default installs of operating systems (Source: SANS G1).
2. Accounts with no passwords or weak passwords (Source: SANS G2).

   Note: Password cracking was not part of our test.
3. Large number of open ports (Source: SANS G4).
4. Not filtering packets for correct incoming and outgoing addresses (Source: SANS G5).
5. Non-existent or incomplete loggings (Source: SANS G6).
6. Vulnerable common gateway interface programs (Source: SANS G7).
7. Scan for malware and other software that can create vulnerabilities (e.g., streaming media) (Source: XACTA).
8. Unnecessary services (e.g., Telnet) (Source: XACTA).

Windows Based Vulnerabilities (NT or 2000 platforms)

9. Unicode (Source: SANS W1).
10. Buffer overflow (Source: SANS W2).
11. IIS RDS exploit (Source: SANS W3).
12. NETBIOS (Source: SANS W4).
13. Information leakage via null session connections (Source: SANS W5).
14. Weak hashing in SAM (Source: SANS W6).
15. Back doors (Source: XACTA).
16. DDOS vulnerabilities (Source: XACTA).

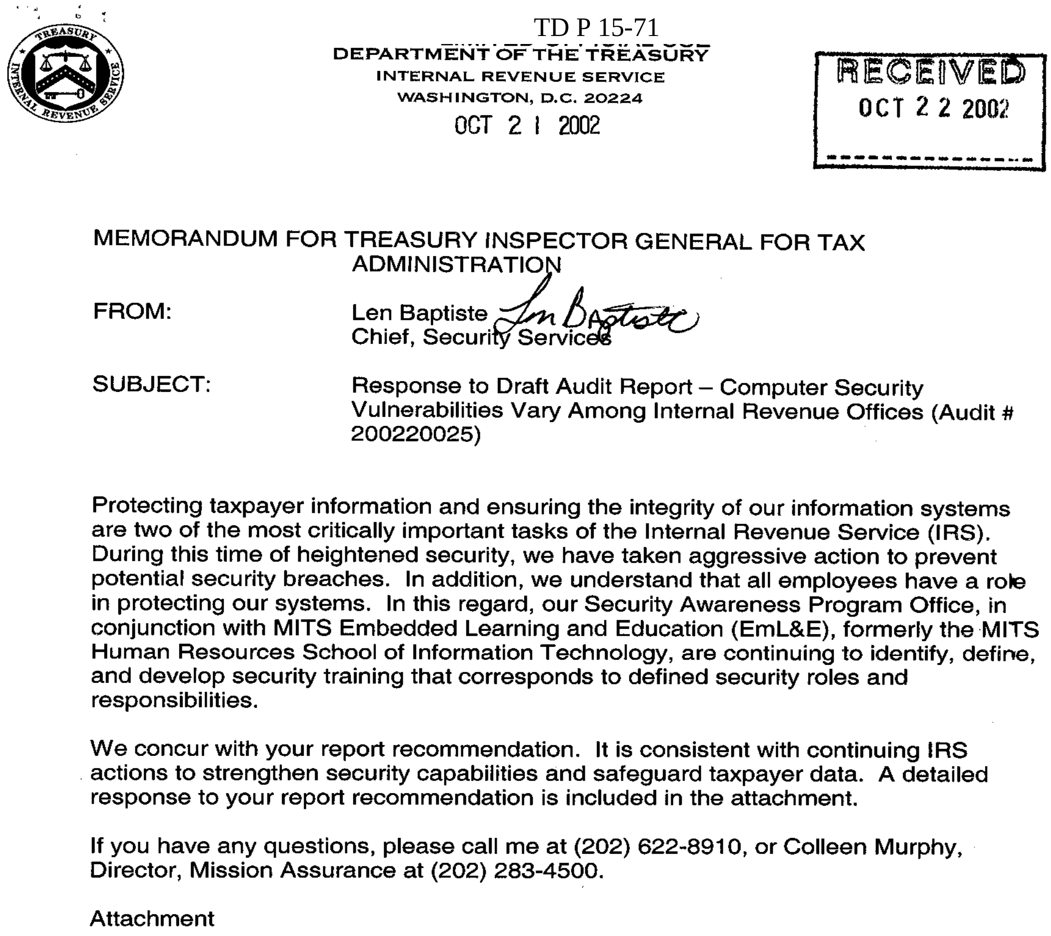
17. Banners (Source: XACTA).

Unix Based Vulnerabilities

18. Buffer overflows in RPC services (Source: SANS U1).
19. Sendmail vulnerabilities (Source: SANS U2).
20. BIND weaknesses (Source: SANS U3).
21. R commands (Source: SANS U4).
22. LPD (Source: SANS U5).
23. Sadmind and mountd (Source: SANS U6).
24. Default SNMP strings (Source: SANS U7).
25. Finger (Source: XACTA).
26. ECHO (Source: XACTA).
27. Shadow file (Source: XACTA).
28. Telnet (Source: XACTA).
29. SSH vulnerabilities (Source: XACTA).

Appendix V

Management's Response to the Draft Report



TD P 15-71

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

OCT 2 1 2002

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Len Baptiste
Chief, Security Services

SUBJECT: Response to Draft Audit Report – Computer Security Vulnerabilities Vary Among Internal Revenue Offices (Audit # 200220025)

Protecting taxpayer information and ensuring the integrity of our information systems are two of the most critically important tasks of the Internal Revenue Service (IRS). During this time of heightened security, we have taken aggressive action to prevent potential security breaches. In addition, we understand that all employees have a role in protecting our systems. In this regard, our Security Awareness Program Office, in conjunction with MITS Embedded Learning and Education (EmL&E), formerly the MITS Human Resources School of Information Technology, are continuing to identify, define, and develop security training that corresponds to defined security roles and responsibilities.

We concur with your report recommendation. It is consistent with continuing IRS actions to strengthen security capabilities and safeguard taxpayer data. A detailed response to your report recommendation is included in the attachment.

If you have any questions, please call me at (202) 622-8910, or Colleen Murphy, Director, Mission Assurance at (202) 283-4500.

Attachment

TD P 15-71

Management response to Draft Audit Report – Computer Security Vulnerabilities Vary Among Internal Revenue Offices (Audit #200220025)

RECOMMENDATION #1: The Deputy Commissioner for Modernization and Chief Information Officer should ensure that:

The system administrators responsible for the equipment in the offices we tested (See Appendix I, Table 4) are given appropriate security training tailored specifically to identifying, assessing, and addressing common security vulnerabilities such as those indicated on the SANS/FBI Top Twenty list. An assessment of whether adequate security training has been provided to systems administrators in other offices should also be considered.

ASSESSMENT OF CAUSE:

Security training relative to system administrator roles and responsibilities has not been clearly defined, and a security training program for system administrators is not implemented Service-wide.

CORRECTIVE ACTION TO RECOMMENDATION #1:

IRS concurs with this recommendation. In conjunction with the IRS material weakness corrective action plan and the Model Facility initiative led by Security Services, activities are underway to identify, define, and develop security training in partnership with the MITS Services Embedded Learning and Education (EmL&E), Information Technology Services, and business units. Barring any shift of resources to address other more time-critical risks, it is anticipated that the following activities will be addressed over the next 18 months.

- Identify security-related training needs to correspond to defined security roles and responsibilities.
- Validate and update current on-line and classroom courses for key personnel.
- Periodically communicate training opportunities and guidance to key personnel.
- Complete development of e-learning tool for key personnel to aid in their understanding of their defined security roles and responsibilities.
- Begin quarterly monitoring of curriculum course participation.

The EmL&E is responsible for tracking employee training, and is improving its ability to identify participation and trends through the service-wide training systems it maintains. Additional employee security training assessment tools and methods will also require coordination with the National Treasury Employees Union (NTEU). The business unit managers are responsible for ensuring that employees receive security awareness training.

IMPLEMENTATION DATE:

April 1, 2004

RESPONSIBLE OFFICIAL:

Director, Mission Assurance, M:S:A

Responsible Partners:
Director, Embedded Learning and Education, M:H
Chief, Information Technology Services, M:I